

UNCLASSIFIED
Cyberspace Human Capital

Air Command and Staff College

Air University

**Cyberspace Human Capital:
Building a Cadre Today to Win Tomorrow's War**



Erica Fountain, Brian Viola & Michael Williams, Major
United States Air Force

A Professional Paper Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Maxwell Air Force Base, Alabama

28 April 2016

1
UNCLASSIFIED

UNCLASSIFIED
Cyberspace Human Capital

DISCLAIMER

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force instruction 51-303, it is not copyrighted, but is the property of the United States Government.

UNCLASSIFIED
Cyberspace Human Capital

Table of Contents

PREFACE

ABSTRACT

INTRODUCTION

DEFINING CYBERSPACE

CYBERSPACE CADRE

DoD Strategic Goal #1: Build and maintain ready forces and capabilities to conduct cyberspace operations.

DoD Strategic Goal #2: Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

DoD Strategic Goal #3: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber[space] attacks of significant consequence.

DoD Strategic Goal #4: Build and maintain viable cyber[space] options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

DoD Strategic Goal #5: Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

CYBERSPACE FORCE MANAGEMENT

ACCESSIONS

RETENTION

INSTITUTIONAL STRUCTURE

FORCE DEVELOPMENT

EDUCATION

TRAINING

FLEXIBILITY

UNCLASSIFIED
Cyberspace Human Capital

PREFACE

We recognize that the scope of any comprehensive overhaul to the current management of cyberspace human capital is extensive. While this paper focuses on the management and development of United States Air Force (USAF) cyberspace officers, it acknowledges the fact that cyberspace operations are inherently joint. And intentionally blurs the lines between the DoD and USAF to highlight this fact. Additionally, we address only USAF officer management and development, consciously abstaining from the needed discussions of sister service cyberspace officers. Finally, this paper's limited engagement with total force cyberspace capabilities is not an assertion that the USAF is the sole cyberspace service. The authors' assertions are blatantly to the contrary: achieving command of the cyberspace domain must be a total-force effort. We would like to thank Col Richard Cooney and Air Command and Staff College cadre for their thoughtful insights and mentorship. All the thoughts herein are our own.

UNCLASSIFIED
Cyberspace Human Capital

ABSTRACT

The Department of Defense relies on cyberspace and the myriad families of systems and networks it supports to deliver decision dominance and battlespace superiority across every warfighting domain. A Revolution of Military Affairs (RMA) is underway in which cyberspace is the key terrain and enables true cross-domain warfare through information operations, network operations, and electromagnetic operations. Furthermore, high-paced technological changes permeate social, political, economic and military spheres, dramatically altering security environments by blurring traditional military, government, commercial and international demarcations. In order to sustain the United States' edge in future conflicts, USAF leadership must develop a sustainable and flexible framework that manages and develops a cyberspace cadre, today and into the future. This professional paper examines USAF and DoD strategic direction and compiles key assertions that will achieve a cyberspace cadre that is joint, flexible and responsive to the challenges ahead. First, the USAF must revisit how it manages and develops cyberspace operators by adapting a functional specific model that mirrors the characteristics of the cyberspace domain (i.e., electromagnetic spectrum, information, network and maintenance aspects) rather than legacy institutional structure. Second, in order to build information age cyberspace human capital, force management principles, which comprise a top-down institutional approach, must be used to determine how and where knowledge, skills, and experience should be distributed across the force of the future. Finally, in order to create a cyberspace cadre that is constantly relevant, force development principles should seek to

UNCLASSIFIED
Cyberspace Human Capital

inculcate bottom-up changes that match specific skills, specialties and classification structures with Air Force missions.



UNCLASSIFIED
Cyberspace Human Capital

INTRODUCTION

“What I fear is not the enemy’s strategy, but our own mistakes.”

—Thucydides, the History of the Peloponnesian War

In the 7th century a revolution in military affairs (RMA) occurred that changed the character of warfare for centuries to follow. The Greek Phalanx took to the battlefield, forming an impregnable wall of heavy infantry, standing shoulder-to-shoulder with tower shields that repelled the most tenacious of attackers. Following the creation of new trade routes and economic prosperity in Greek city-states like Corinth, Thebes and Athens, access to new resources transformed how weapons were formed and how war was fought. Iron replaced bronze as the primary material for weapons, allowing soldiers to equip sturdy helmets, armor and shields. Additionally, groups of soldiers became more disciplined, forming battle lines that enabled formational attack and defense. Prior to this innovation, military activity of the Bronze Age was a matter of aristocratic warriors, pitched in single man-on-man combat. The Greek art of war and the Phalanx transformed warfighting into a well-orchestrated system of offensive capability and tactical mobility.

Today, another Revolution of Military Affairs (RMA) is underway: information operations, network operations, electromagnetic operations and integrated Command, Control, Communications and Computer systems fused with Intelligence, Surveillance and Reconnaissance systems (C4ISR) have become the hallmarks of America’s future warfighting

UNCLASSIFIED
Cyberspace Human Capital

dominance.¹ In order to sustain the United States' edge in future conflicts USAF leadership must develop a sustainable and flexible framework that manages and develops a highly capable cyberspace cadre.

In the current RMA, technological automation, distributed computing and battlespace agility supersede industrial might, monolithic systems and massive firepower in the ongoing revolution. Additionally, high-paced technological changes continue to permeate social, political, economic and military spheres, dramatically altering security environments. Leaders in the Department of Defense (DoD) must have the foresight to comprehend and adapt to dynamic changes that continuously alter the strategic landscape. The inability to learn (e.g., lessons from organizational deficiency), to anticipate (e.g., understanding the new nature of war or technology) or to adapt (e.g., inherent reluctance of human behavior manifested in institutional rigidity) causes organizational failure.² Therefore, in order to sustain momentum through the present RMA, insightful leadership is fundamental to gauging the complex mix of tactical, organizational, doctrinal and technological innovations ahead and leading the force to new conceptual approaches to warfare.³ Bold leadership that is adaptive and responsive to the unfolding complexities ahead is paramount to leading at the edge of the current revolution in military affairs.

¹ SecDef Memo on the Defense Innovation Initiative, 15 Nov 2014

² Wood Lecture

³ Murray and Knox, *The Dynamics of Military Revolution: 1300-2050* (New York: Cambridge University Press, 2001);

UNCLASSIFIED
Cyberspace Human Capital

The key terrain of the present RMA is the cyberspace domain. Cyberspace threads the air, land, sea and space domains together, creating an integrated layer of joint-force effectiveness.⁴ Without exception, every component of America's military force entrusts mission assurance to this highly contested domain. Furthermore, the cyberspace domain provides potential adversaries with a low-cost means to undercut US military effectiveness.⁵ Deny, degrade, disrupt, deceive and/or corruption of cyberspace key terrain (CKT) dangerously alters the strategic context and erodes US warfighting dominance. The terrain enables adversarial strategies like cyberspace denial operations, espionage activities and anti-access/area-denial (A2/AD) strategies, turning traditional mass and maneuver on its head. Counter to traditional warfighting doctrine, mass in cyberspace is potentially disadvantageous to operations: mass in cyberspace expands the attack surface we present to our adversaries. If current trends hold, state and non-state actors will continue to develop and modernize capabilities that degrade DoD mission assurance across all warfighting domains, especially in areas where the United States has historically retained exclusive superiority (e.g. air superiority, space, etc.). Cyberspace leaders of the future must recognize that even while cyberspace multiplies joint force capabilities, adversaries will tenaciously pursue asymmetric strategies through cyberspace, which will continue to deepen in sophistication and intensity.⁶ The functional management of cyberspace is the ideal framework to address the strategic landscape of this environment.

⁴ Brig Gen Sarah Zabel, Cyber in Mission Assurance, A White Paper, 10 June 2015

⁵ Adm Rogers USCYBERCOM Statement, HASC, 4 March 2015

⁶ Adm Rogers USCYBERCOM Statement, HASC, 4 March 2015, 10

UNCLASSIFIED
Cyberspace Human Capital

DEFINING CYBERSPACE

The most comprehensive, and consequently the most useful, definition of cyberspace is the one provided by the 2006 National Military Strategy for Cyberspace Operations: “Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”⁷ Though there are more recent definitions, they often skew focus to Network Operations (NetOps). This is arguably a result of NetOps encompassing the preponderance of current operations; however, this is myopic as it prevents the USAF from shaping cyberspace human capital to meet current and future needs. Furthermore, the word “cyber” has become the buzzword of the 21st century and the DoD has latched onto it with intense fervor. Initially, cyber was simply the truncated version of cyberspace; however, its wide-ranging use has lately added more uncertainty than clarity to the dialogue. To avoid such ambiguity, this paper refrains from using the general term of cyber. Rather, the term cyberspace is used when referencing domain and the terms NetOps, Electromagnetic Operations (EMO), Information Operations (IO), and Maintenance (Mx) Operations when referencing functional aspects.

The one-size-fits-all use of cyber simply does not work. Similarly, the current broad cyberspace officer bucket does not provide adequate granularity to manage cyberspace forces. In order to provide the necessary fidelity, a management framework based on the functional principles of the domain is necessary. A 2007 report to congress by the Congressional Research Service amplifies this view by specifying five core cyberspace capabilities: (1) psychological

⁷ National Military Strategy for Cyberspace Operations, 15

UNCLASSIFIED
Cyberspace Human Capital

operations, (2) military deception, (3) operations security, (4) computer network operations, (5) electronic warfare (EW).^{8,9} Psychological operations and military deception fall under information operations functions, operations security (DCO) and computer network operations (OCO) are network operations functions, and EW is a EMO function. Leveraging this perspective, the cyberforce human capital framework is composed of four primary functional areas: electromagnetic operations, network operations, information operations, cyberspace maintenance.¹⁰ Though their application within the cyberspace domain may change over the course of time (or new functional areas emerge), this approach provides the USAF the best mechanism to cope with the ever-changing cyberspace landscape. It addresses cyberspace doctrine while providing the fidelity necessary to build actionable cyberspace human capital plans.

EMO are operations that occur by exploiting the characteristics of the Electromagnetic Spectrum (EMS). The emergence of the cyberspace domain drove the broadening of the EW discipline into electromagnetic operations. As outlined in the DoD's Electromagnetic Spectrum Strategy (EMS), 2013, "adversaries are aggressively fielding electronic attack and cyber[space] technologies that significantly erode [the] DoD's ability to use the spectrum to conduct military operations."¹¹ Per JP 3-13.1 electronic warfare is "waged to secure and maintain the freedom of action in the electromagnetic spectrum."¹² The EMS is the intersection of the cyberspace and

⁸ 2007 CRS Report to Congress, pg. 3

⁹ Joint Pub 3-13, Information Operations, November 2012, pg. X, I-3.

¹⁰ [Recommendation R1](#): Revise the definition of cyberspace to address four functional areas.

¹¹ DoD, Electromagnetic Spectrum Strategy 2013, September 2013.

¹² Joint Pub 3-13.1, Electronic Warfare, January 2007. pg. V.

UNCLASSIFIED
Cyberspace Human Capital

sea, land, air and space domains. Whether it is radio waves traveling through air and space, light traveling through subsea fiber optic cable, or raw data at rest on magnetic media, EMS is the physical representation of the cyberspace domain. In order to ensure that the USAF's cyberspace force of the future is able to provide the essential capabilities to ensure mission success, EMO is a core function of the cyberspace domain.

NetOps are operations that occur by exploiting the characteristics of the logical layer of cyberspace. The core of the cyberspace domain is digital data, virtual paths and mechanisms. Effects are achieved through the denying, disruption, degradation, destruction, deception, manipulation and/or corruption of data at rest or in motion, or digital manipulation of infrastructure.¹³ For this reason, NetOps is another key functional area of the cyberspace domain.

IO are “[t]he relational framework [which] describes the application, integration and synchronization of [information related capabilities] IRCs to influence, disrupt, corrupt, or usurp the decision making of a [target audience] TA to create a desired effect to support achievement of an objective.”¹⁴ The general understanding is that IO broader than just the cyberspace domain; cyberspace increasingly allows for the propagation of information across the globe at an accelerated pace, which enable IO and effects. It is likely that IO, within and through the cyberspace domain, will overshadow all other forms of traditional IO in the near future. Controlling the narrative within and through cyberspace is imperative to all military operations. Additionally, it is highly likely that the DoD will rely on IO, dovetailed with cyberspace

¹³ Joint Pub 3-12, II-5

¹⁴ Joint Pub 3-13, Information Operations, November 2014. pg. X.

UNCLASSIFIED
Cyberspace Human Capital

operations, to support all US Instrument of Power (IOP) efforts. As the Information Ops 14F career field completes its transition through 2016, there is opportunity for cyberspace operations officers to create some very unique effects. For these reasons, and in order to enable multi-domain synergy, IO is also a core functional area of the cyberspace domain.

Cyberspace maintenance are functional operations that build, sustain, and standardize the CKT by providing the physical environment (e.g., infrastructure) for cyberspace operations (EMO, NetOps, IO) as well as the AFIN (Air Force Information Networks). The AFIN is the globally interconnected, end-to-end set of AF unique information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. The AFIN can be considered the networked USAF Information Environment.¹⁵ It is typically referred to using the legacy moniker Communications and Information (C&I) as it broadly covers many aspects not strictly operational in the truest sense. It also encompasses activities like Combat Communications and AOC Communications. Cyberspace maintenance creates, manages and sustains the circuit and must therefore be treated as a core functional area of the cyberspace domain.

¹⁵ AFI 33-115 16 SEPTEMBER 2014, AFIN Defined

UNCLASSIFIED
Cyberspace Human Capital

CYBERSPACE CADRE

Fortunately, senior leaders in our nation and USAF are aware of the challenges ahead. They see a necessary transformation on the horizon that will require bold changes to traditional missions and the force of the future. In 2008, Secretary of the Air Force Donley and Chief of Staff of the Air Force, General Schwartz, kick-started the transformation of the USAF's foundational mission imperatives with a new mission statement: "to fly, fight and win in air, space and cyberspace."¹⁶ New attitudes about how cyberspace relates to USAF missions are a premium in gauging the future.¹⁷ Additionally, senior leaders in the DoD must increase their focus on efforts that develop a cyberspace cadre that is ready to achieve the vision described in the DoD's Strategy for Cyberspace: defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace.¹⁸ Lastly, a well-developed cyberspace human capital plan underscores the cyberforce of the future and unlocks lines of effort in-synch with DoD Strategic Goals.

DoD Strategic Goal #1: Build and maintain ready forces and capabilities to conduct cyberspace operations.¹⁹

DoD Strategic Goal #2: Defend the DoD information network, secure DoD data, and mitigate risks to DoD

¹⁶ SECAF Donley and CSAF Schwartz comments at AFA, 2008

¹⁷ Brig Gen Sarah Zabel, Cyber in Mission Assurance, A White Paper, 10 June 2015

¹⁸ DoD Strategy for Cyberspace Operations (2015)

¹⁹ Neither education nor training alone will adequately provide the DoD the cyberspace cadre of the future. Developing the cadre of the future requires a holistic approach that accesses the right Airman-leaders and develops and retains hard-won skills through both leadership and technical tracks.

UNCLASSIFIED
Cyberspace Human Capital

missions.²⁰

DoD Strategic Goal #3: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or

destructive cyber[space] attacks of significant consequence.²¹

DoD Strategic Goal #4: Build and maintain viable cyber[space] options and plan to use those options to control

conflict escalation and to shape the conflict environment at all stages.²²

DoD Strategic Goal #5: Build and maintain robust international alliances and partnerships to deter shared

threats and increase international security and stability.²³

In the context of DoD Strategic Vision for Cyberspace, the central question becomes:

how does the USAF develop and manage the current and next generation of cyberspace officers in order to meet today's mission requirements while building tomorrow's cyberspace force of the future? This paper addresses this question along two lines of effort: force management and force

²⁰ Cyberspace is inherently joint. Each branch of the U.S. military is expected to work together over a common domain in order to maximize success of cyberspace operations. Therefore, joint-mindedness and inter-service coordination must be primary lines of effort in developing future cyberspace cadre.

²¹ Mission assurance requires whole-of-government approaches, engagement with industry partners, as well as unlocking potential in the Air National Guard and Reserve Force. Future cyberspace cadre must have the flexibility to coordinate missions across these layers to guarantee cyberspace superiority.

²² Senior leaders need options that respond to, deter and defeat adversarial actions. Future cyberspace cadre must be able to gauge the depth and breadth of friendly and adversarial actions in cyberspace and convey ideas to senior leadership in a manner that is meaningful and presents a spectrum of options.

²³ Allies possess complementary capabilities that can augment those of the DoD and can be used to strengthen alliances, sending a strategic message of deterrence and collective defense. Future cyberspace cadre will be prime-movers in these partnerships and must be able to collaborate with allies in a manner consistent with national strategy.

UNCLASSIFIED
Cyberspace Human Capital

development. Force management is primarily a top-down institutional approach that determines the necessary capabilities for the force of the future and how knowledge, skills and experience are distributed.²⁴ Force development, on the other hand, is primarily bottom-up in that it seeks specific skills, specialties and classification structures necessary across the active duty and civilian force that leads to a viable cyberspace force.²⁵

CYBERSPACE FORCE MANAGEMENT

The USAF's vision for integrating cyberspace capabilities will ultimately define how it will operate in cyberspace now and into the future.²⁶ Force management efforts address both functional aspects (EMO, NetOps, IO and Maintenance) as well as continuously making organizational adjustments that keep pace with the information age. The USAF must continue to build knowledge, skills, and experience to execute cyberspace missions in each of the four functional areas,²⁷ while scrutinizing each strata of the cyberspace officer cadre in order to determine the education, training and experiences necessary to confront the nation's adversaries today and into the future. Long-term projections must capture the next generation of cyberspace operations officers and incentivize retention of existing talent cultivated through the ranks.

A functional approach to management overcomes many of the long-term challenges in “operationalizing” the cyberspace career field. Beginning in 2008, USAF discussions about cyberspace dominance reached fever pitch with the creation of the 24th Air Force as the

²⁴ Rand, Human Capital Management for the USAF Cyber Force, viii

²⁵ Ibid.

²⁶ Rand, Human Capital Management for the USAF Cyber Force, vii

²⁷ 2015 DoD Cyber Strategy

UNCLASSIFIED
Cyberspace Human Capital

warfighting headquarters to provide combat-ready cyberspace forces.²⁸ In order to transition from cyberspace support to operations, in 2010 the communication and information (C&I) officer career field (33S) was “operationalized” into the cyberspace operations officer. The year 2011 saw the first critical step in developing a cyberspace force of the future with the creation of Undergraduate Cyberspace Training (UCT) at Keesler AFB, MS.²⁹ Then, beginning in 2013, the Air Force and sister services began a “surge” to bring cyberspace mission force capability to bear for USCYBERCOM. In 2014, a “pseudo-split” in the 2,500 member 17D career field created a new branch (as a subset) of 17D dubbed 17S, or Cyberspace Warfare Officers (CWOs). This new subset is yet another well-intentioned effort to operationalize the career field, while retaining a broad workforce to complete a wide variety of legacy C&I missions. While this capability focused approach addresses some of the ailing symptoms of the 17D career field, it falls short in addressing the long-term challenges posed by the cyberspace domain. Additionally, internal factors have limited the USAF’s efforts to tackle the long-term human capital problem: DoD-level reductions in force, an identity crisis stemming from a sudden start into operations, and an inability to balance a diverse career field that had to learn - literally overnight - what it means to conduct operations while continuing to perform legacy C&I functions. Managing the career field through its functional areas (i.e., NetOps, EMO, IO, and Maintenance) allows management fidelity while promoting an agile framework responsive to future and emerging mission requirements.

²⁸ Rand, Human Capital Management for the USAF Cyber Force, 1

²⁹ <http://www.afspc.af.mil/news/story.asp?id=123255758>

UNCLASSIFIED
Cyberspace Human Capital

At its core, the goal of force management is to infuse the right amounts of knowledge, skills and experience (through education and training) at key trigger points during every officer's career. Functional force management actions focus on "what" capabilities are required for current and future mission sets (e.g., the education, training and career flexibility) as well as the "how" (e.g., force size considerations, obtaining/retaining and developing talent, managing corporate knowledge, and removing barriers to the health of the force). By mapping out milestones that encompass leadership opportunity, management experience, developing warrior ethos and joint integration, force management paves the way for the cyberspace force of the future. The overarching goal is to make the *right* investments today in human capital, thereby building and sustaining a relevant workforce for current and future operations. Functional force management functions are explained by three major area lines of effort: accessions, retention and institutional flexibility.

ACCESSIONS

The long-term challenge of building cyberspace human capital begins by opening the tap to the future force. As the USAF garners the cyberspace force of the future it must deliberately make visceral connections with the current generation of digital natives who intuitively navigate the high-tech cyberspace domain. The USAF has a lot to offer new recruits interested in cyberspace operations. The USAF offers leadership opportunity, teamwork and esprit de corps not inherent in many other lines of work, especially in the civilian world. USAF cyberspace officers have the opportunity to solve complex problems, conduct novel operations and defend

UNCLASSIFIED
Cyberspace Human Capital

the nation against, and with, cutting-edge technologies. Traditional means of attracting talent (e.g., USAF recruitment via social media, television and/or streaming media) continue to be effective means for gaining the attention of a generation that is looking for a higher calling. However, accession tools must be agile to serve the interests of qualified graduates that possess both aptitude and affinity, while tailorabile to shape accessions within a changing landscape.³⁰

Science, Technology, Engineering and Math (STEM) degree, combined with aptitude, affinity, and professional certification(s) make up one composite sketch of tomorrow's cyberspace officer corps. However, while STEM certainly prepares cyberspace operators with formal baseline skills, it also shouldn't bound accession efforts: if potential candidates demonstrate both aptitude *and* affinity, exceptions should be made to acquire talent. Furthermore, technology drives the cyberspace domain, and consequently, it is vital that future cyberspace officers have a solid grasp of domain fundamentals. Therefore, accession efforts must connect with potential graduates who have the right aptitude *and* affinity to succeed in rigorous cyberspace operations assignments.³¹ Lastly, engaging the current generation with a viable career path that marries individual interests with national security is a critical balance. STEM educational requirements are covered more in depth in the Force Development section of this paper. There are a few ideas that could significantly improve the input flow of cyberspace talent:

³⁰ Lara Schmidt, Perspective on 2015 DoD Cyber Strategy

³¹ [Recommendation R2](#): Revisit entry requirements by assessing aptitude and affinity as equal indicators of career success.

UNCLASSIFIED
Cyberspace Human Capital

- 1) Making concerted efforts across all our nation's universities that engage with the educators themselves can amplify the recruitment message of the USAF.³² A DMDC strategy report found that recruiting efforts could be improved by increasing educators' understanding of the military and fostering a more positive attitude toward military service. By offering site-visits, augmenting educator personal interests in military and/or partnering strategies with educators can enhance recruitment efforts.³³
- 2) The National Security Agency has designated 44 colleges as those with demonstrated academic institutional excellence in applying the academic rigor necessary to produce students with superlative skills in information assurance, cyberspace research and network defense.³⁴ By focusing efforts (e.g., marketing, capability demonstrations) at these institutions, the USAF can gather a junior force with the right background to guarantee success.³⁵
- 3) Alumni profiles are an effective means of telling the story.³⁶ By sharing the success stories of alumni (who have attended the targeted university), a connection is established that creates a bond of shared heritage. By connecting those currently serving with those considering service, the USAF can potentially create more open doors to those who have trepidation about military service.

³² [Recommendation R3](#): USAF pursue educator investment strategies that amplify recruitment capabilities.

³³ Anita R. Lancaster, Elaine Sellman and Julie Hasset. The Educator Market: Military Recruiting Strategies, Aug 2002

³⁴ NSA National Centers of Academic Excellence in IA/CD, link:
https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

³⁵ [Recommendation R4](#): Target NSA academic excellence institutions for accessions

³⁶ [Recommendation R5](#): Cyberspace alumni profiles in college publications

UNCLASSIFIED
Cyberspace Human Capital

- 4) Tailored scholarships can acquire the right talent for the force of the future. Rather than recreate the existing robust civilian education system, the USAF should focus on precise tailored recruiting. On average the USAF commissions 175 new cyberspace officers per year through ROTC. As of 2013 the National Center for Education Statistics reported the average annual tuition cost to be \$34,483 per year. Using this somewhat dated gauge, the cost of providing tailored scholarships to 75% of those accessions would be roughly \$4.2M annually. Cyberforce scholarships should be distributed to forecast the growth of core functional areas.³⁷ Additionally, scholarships must require concentration areas of study based on the tailored educational needs of each functional area. Finally, scholarships awardees can be earmarked for outplacement into a specific functional area, providing a tailor-made tool to adjust force of the future capability shortfalls.
- 5) Capabilities testing - both aptitude and affinity - must ensure that the right baseline individual enters service. An “AFOQT-like” test could determine whether student desires match capability. Additionally, an affinity test could determine whether student capability matches the fast-paced nature of the cyberspace career field.

RETENTION

If acquiring those with the right talent to succeed as part of the USAF’s cyberspace force of the future is the first major challenge, then retaining that talent is the next. Leadership must continue to have a watchful eye for those who can solve the service’s thorniest cyberspace

³⁷ [Recommendation R6](#): Develop scholarships which require concentration on areas of study with earmarked outplacement into a specific functional area.

UNCLASSIFIED
Cyberspace Human Capital

issues, communicate with senior leadership across DoD, and mentor the next generation of cyberspace leaders. Nurturing these skills take time, money and patience. Retaining knowledge, skills, and experience of the cyberspace force is an imperative for successful cyberspace operations, now and into the future.

Motivating Airmen to continue service is the most critical task in sustaining human capital for the cyberspace force of the future. Often, Airmen find it frustrating to become a cyberspace officer, only to find out that after one or two tours in an operational position, they are forcefully moved to a non-operational desk position. Unfortunately, moves of this nature injure hard-won skills, squander leadership opportunity and diminish the operational mindset the USAF hopes to instantiate in the mind of cyberspace cadre. To make matters worse, this often happens right at the first voluntary continuation opportunity (~4 years), heavily influencing the person's decision to stay or to seek commercial employment. Building a cyberspace officer takes time and financial investments similar to pilots. Additionally, competition with private industry and the commercial sector is high, making it difficult to retain cyberspace officers with STEM degrees and technical expertise. This effect is exacerbated by the DoD conversion of operational cyberspace jobs from uniformed members to contractors. Despite the challenges in retaining cyberspace talent, there are numerous considerations that will alleviate the stress on the career field.

Retaining the cyberspace force of the future is predicated on building long-term relationships of trust with cyberspace officers across all strata of the force. There are lessons the USAF should borrow from commercial sector enterprises that have been in strident competition

UNCLASSIFIED
Cyberspace Human Capital

for the dwindling cyberspace talent pool. A recent RAND study found that the commercial sector's ability to retain skilled personnel is closely linked to job satisfaction, through good working environments, belief in the mission, opportunities for training and professional development, and access to interesting assignments.³⁸ For instance, building on the premise that the USAF desires to draw those with an affinity for technology, supporting life-long passion for technology encourages innovation and develops mutual trust.³⁹ Cyberspace is a community of expertise that extends far beyond the individual.⁴⁰ High performers must be given opportunities to participate and to contribute to technology boards, conventions, conferences and working groups.⁴¹ These provide two long-term benefits: connecting the officer to the broader field of activity he/she is interested in and creating important community associations with industry, government and international partners. In return, the USAF retains an officer with broadened social connections that amplify his/her capability to solve tough problems. Additionally, developing a selective USAF conference, modeled after the Intelligence Communities (IC) CNEDEV or civilian events like BlackHat, ShmooCon, CanSecWest, and DEFCON sends a strong message to cyberspace Airmen that their talents are valued.⁴² By fostering opportunities to explore new technologies and exposing officers to new concepts, the USAF gains a broadened officer with more tools that can help solve critical problems.

³⁸ Lara Schmidt, Perspective on 2015 DoD Cyber Strategy

³⁹ [Recommendation R7](#): Retain cyberspace operations officers by supporting technology passions.

⁴⁰ James Kaplan, Naufal Khan and Roger Roberts. [Winning the Battle for Technology Talent, Business Technology Office](#), 2012.

⁴¹ [Recommendation R8](#): Retain cyberspace operations officers by facilitating exposure opportunities

⁴² [Recommendation R9](#): Develop a selective USAF cyber-conference

UNCLASSIFIED
Cyberspace Human Capital

Retaining a diverse force of the future is also predicated on the USAF's ability to revise typical promotion paths.⁴³ By comparison, successful corporate retention programs seek to provide satisfying career paths for their cyberspace workforce, including tracks for promotion through both management and technical tracks (see [Figure 1](#)).⁴⁴ Unfortunately, the USAF continues to reinforce a single mold career track that prejudices promotion opportunity to those who follow the "standard pyramid" track to the top. To Airmen, promotions are a primary indication that his/her skills are valuable and he/she is intrinsically important to the mission. By using a multi-path construct, levying increased responsibility and tiered financial "in-rank" incentives signals Airmen that their skills and abilities are valued. Comparable to the cost and time required to become proficient in an airframe, cyberspace Airmen must be empowered to nurture proficiency through the first ten years of service (see [Figure 1](#)).⁴⁵ If Airmen know they have options that meet both their personal and professional goals then they are more likely to continue service. This 10-year milestone becomes the first opportunity for willing cyberspace officers to transition to positions that begin to build the breadth necessary for traditional senior leadership roles. If a cyberspace officer chooses the technical track, it is not to say that leadership opportunities are non-existent. Rather they are more mission focused, taking the form of mission or crew commands. While this track is technically rewarding, it lacks monetary incentives; in order to financially bridge the divide between a traditional leadership track officer advancing through the ranks and/or industry, the USAF must incentivize those Airmen through a

⁴³ [Recommendation R10](#): Revisit/revise career path (pyramid) tracks for cyberspace officers.

⁴⁴ Lara Schmidt, Perspective on 2015 DoD Cyber Strategy

⁴⁵ [Recommendation R10](#): Revisit/revise career path (pyramid) tracks for cyberspace officers.

UNCLASSIFIED
Cyberspace Human Capital

tiered, “in-rank” bonus system, much like the steps of the civilian General Schedule (GS) system.⁴⁶ Alternatively, cyberspace officers who prefer the management track will have broader based opportunities to lead through squadron, group or wing command opportunities, following traditional promotion systems. Cyberspace officers who take this track may find themselves performing a variety of tasks, such as special duty, career broadening, or serving on a MAJCOM or Joint Staff. While less technical in nature, it provides Airmen broad career mobility that many seek after the 10-year milestone. Bottom line, the career field must encourage an ethos that does not discourage career broadening opportunities that are not in line with a perceived promotion path. There is no one path to promotion; career broadening creates well-rounded, adaptable cyberspace leaders. Failing to rethink promotion paths will continue the exodus of talent the USAF cannot afford.

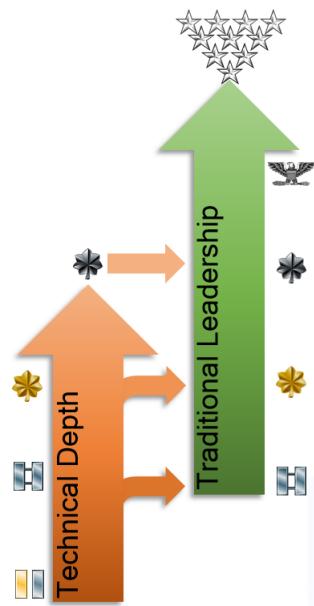
Digital Collections
Air University Maxwell Air Force Base

In order to ensure that high performing, cyberspace officers within other career fields are retained, we must encourage crossflow opportunities where it makes sense. The crossflows should not be driven by bodies and billets but rather by records, volunteers and a rigorous testing effort (aptitude and affinity). These methods ensure selection of Airmen with only the highest affinity, aptitude and officership qualities. For example, the Computer Network Operations Development Program (CNODP) program is arguably recognized as the DoD's top program for

⁴⁶ [Recommendation R11](#): Develop a tiered “in-rank” bonus system to encourage continuation of service along technical tracks.

UNCLASSIFIED
Cyberspace Human Capital

NetOps development. It consists of a three-year internship and a \$375K investment. Historically, 62 officers compose roughly 50% of graduates and have excelled compared to cyberspace officers with STEM degrees and arguably outperformed those without such degrees. Unfortunately, currently there is no path for 62 graduates that continue to excel within cyberspace operations to crossflow into the cyberspace operations community. As a consequence, 49% of 62 CNODP graduates separate upon completion of their commitment: an attrition of talent which could be drastically curtailed by simply opening crossflow opportunities.



Lastly, it is critical to understand the reasons why cyberspace officers leave (e.g., job satisfaction, pay, value to the organization). Highly skilled cyberspace officers will often separate from the military only to do the same job for the military as a contractor with higher pay, without the officership overhead. This exodus of hard-won talent erodes the USAF's organic knowledge base. A formalized exit interview process creates a data mine that can be harvested to create a feedback loop, informing senior leaders regarding health of the cyberforce.⁴⁷

⁴⁷ [Recommendation R12](#): Conduct exit interviews to discern causal factors for cyberspace operations officer separations

UNCLASSIFIED
Cyberspace Human Capital

INSTITUTIONAL STRUCTURE

If the USAF is committed to addressing the human capital issues it faces, it must adopt a whole-of-DoD approach to ensure its success. This can be accomplished because of the numerous synergies among the active duty, Air National Guard and Reserve forces as well as acknowledging the congruences in cyberspace operations between each of the DoD components. Additionally, it must become whole-heartedly committed to iterative advancements and continuous lateral movements within the cyberspace cadre. Attacking the human capital issue for the force of the future includes resisting the temptation to focus singularly on cyberspace officers, but must encompass regions of activity that can dovetail across Title-10, -32, -50 lines, agency activities and service competencies.

First, senior leadership must provide direction that reflects future DoD and service priorities (as can be best approximated). Joint warfighting in cyberspace is a quality that must be developed in the USAF's cyberspace cadre.⁴⁸ The USAF is currently committed to seven cyberspace protection teams (CPTs) as part of the cyberspace mission force (CMF). This is a significant signpost for future operations that the USAF must pay attention to: cyberspace is inherently joint and each service must cooperate to develop synergy through multi-domain effects, amplifying individual service capabilities. Joint doctrine treats cyberspace as a critical warfighting capability that will be used in conjunction with other warfighting capabilities.⁴⁹ Additionally, SAF/CIO's tenets of information dominance acknowledge that, "...there exists a

⁴⁸ [Recommendation R13](#): Cyberspace operations officers require exposure to joint environments early in their careers.

⁴⁹ Joint Publication 3-12, Cyberspace Operations

UNCLASSIFIED
Cyberspace Human Capital

multi-domain approach to [cyberspace] operations that increases the effectiveness of Air Force core missions.⁵⁰ Naturally, as each service commits cadre to joint operations in cyberspace (especially as through the CMF), it is highly likely that Airmen will be tasked to conduct cyberspace operations in support of sister services. Cyberspace, whether Army, USAF, Navy or Marine Corps, is a uniform-agnostic operational domain. Therefore, it's not a far stretch to imagine that a soldier, sailor or marine may be required to perform cyberspace tasks in support of USAF operations. The USAF must always have an eye toward developing Airmen with joint experience as a priority. Opportunities to build joint knowledge, skills and experience should happen well before the Airman is a major.

Second, the USAF must continue to capitalize on the extant institutional cyberspace talent-pool. Presently, Airmen from other career paths, such as space operations (13S), developmental engineering (62E/C), intelligence (14N) and acquisitions management (63A) fill some of the most demanding cyberspace operations jobs. However, some career field functional managers restrict the infusion of cyberspace talent by erecting barriers through institutional personnel systems and processes. Low manning levels in some AFSCs drives an institutional bean-counting approach that prevents matriculation of talent needed at the middle levels of cyberspace operations (Captains to Lieutenant Colonels). This prevents the logical flow of available skills to much more critical areas. By fast-tracking Airmen with cyberspace skills from other career fields in critical cyberspace jobs, the USAF will foster innovation, depth and breadth

⁵⁰ Air Force Information Dominance Flight Plan, The Way Forward for Cyberspace/IT in the United States Air Force, May 2015

UNCLASSIFIED
Cyberspace Human Capital

of knowledge, and enhance support to USAF core missions.⁵¹ Knowledge, skills, and experience must outweigh the judgments of those operating institutional personnel systems. By removing these long-standing institutional barriers, the USAF can optimize the talent that is already resident in its ranks.

Third, Total Force Integration (TFI) is an oft-overlooked capacity that the USAF can lean on to plus-up its human capital. The Air National Guard (ANG) and USAF Reserves bring unique experiences and niche capabilities to bear that can help sustain the USAF for the long-term. For instance, the 262d Network Warfare Squadron (NWS) in Seattle (which includes Airmen who also work with Microsoft) and the 175th NWS at Fort Meade (who are embedded in NSA) are just a few examples of unique knowledge, skills and experience that can broaden the force of the future.⁵² Units like Vermont's 159th Fighter Wing's Cyber Guard are models for filling capability gaps where needed: developing courses for the 39th Information Operations Squadron (IOS) and Cyber 200 at Wright-Patterson AFB. Additionally, because many of the guardsmen and reservists have previous active duty experience and leadership ability, cross-flow opportunities through the Captain and Major ranks might augment shortfalls in the active duty force from members who have voluntarily left service at the 4-year or 8-year marks. All things considered, the ANG/Reserves are another vein of talent that the USAF must continually tap as it digs toward understanding the requirements for a force of the future.⁵³

⁵¹ [Recommendation R14](#): Lower barriers to crossflow for those with requisite cyberspace knowledge, skills and experience.

⁵² Sidney Freedburg, [National Guard Fights for Cyber Role in 2015 Budget](#), Breaking Defense, Feb 15

⁵³ [Recommendation R15](#): Leverage human capital across the ANG/USAF Reserves to maximize force capabilities

UNCLASSIFIED
Cyberspace Human Capital

Lastly, iterative approaches and recurring round-tables must be common themes in the discussion. Because of the uncertain nature and unclear requirements for cyberspace capabilities in the future, USAF leadership must be willing to continually engage members within its ranks to assess the health of the force. Additionally, senior leadership must continue to give direction regarding the force management priorities of the force by treating roadmaps and flight-plans as living documents in order to solicit feedback from the force. Working groups at the corporate HAF-/SAF-level must sponsor dialogue between force management, force development components of the active duty, ANG, USAF Reserves on at least an annual basis. Partnerships with other services, academia and industry will be key to developing a sustainable force development plan that maximizes human capital.

FORCE DEVELOPMENT

The most critical weapon in our cyberspace arsenal is our Airmen. Thus, it is paramount that we develop our cyberspace officers to maintain our edge in current operations and in future capabilities. The overall goal of Cyberspace force development is deliberately ensuring the professional development of cyberspace officers, tailored to meet joint and USAF warfighting requirements. This is accomplished by developing Airmen with the skills, training and experience to lead current and future mission requirements. RAND observed in 2010 that most airmen are developed for “cyber-hybrid” jobs (i.e. jobs that require both traditional C&I skillsets as well as specialized cyberspace warfare skillsets) through organizationally specific on-the-job

UNCLASSIFIED
Cyberspace Human Capital

training programs.⁵⁴ This training results in just-in-time cyber skills for just enough cyber personnel. Because we estimate that about 2,600 cyber-hybrid jobs exist throughout the USAF, we believe that a decentralized, organizationally specific development approach is not enough to build a sustainable cyber workforce.

As Lieutenant General William Lord, former USAF Chief of Warfighting Integration and Chief Information Officer, rightly observed, “the Air Force’s cyberspace operators must focus on operational rigor and mission assurance in order to effectively establish, control and leverage cyberspace capabilities.”⁵⁵ To establish this focus, it is essential for cyberspace officers to have a solid grasp on domain fundamentals through education and training. Education and training facilitate the transition from one level of experience to the next and are critical to creating productive experiences in a cyberspace officer’s development. There is a clear distinction between these two concepts. Training provides cyberspace officers with proficiency on current practices, whereas education builds a foundation that prepares officers to deal with the unknown art of cyberspace operations and uncertain future challenges.

EDUCATION

Education is of vital importance to the cyberspace career field. Education focuses on developing critical thought that enables successful creative solutions to new problems. If we assume that as technology progresses and automation continues at its current pace (e.g., man-in-

⁵⁴ Rand, Human Capital Management for the USAF Cyber Force, ix

⁵⁵ Lieutenant General William Lord, [New Air Force Cyberspace Badge Guidelines Released](#), Apr 10

UNCLASSIFIED
Cyberspace Human Capital

the-loop⁵⁶ vs. man-on-the-loop⁵⁷ decision systems) then perhaps education deserves greater emphasis in order to best arm today's cyberforce and conquer tomorrow's mission set, it is essential that a premium is placed on the STEM disciplines. As Jabbour and Kline emphasize, education exerts the cognitive dimension of thinking (open system) while training emphasizes the psychomotor part (closed system).⁵⁸ Technology will continue to drive the evolution of cyberspace. A cyberforce built upon the STEM disciplines is trainable to adapt to tomorrow's challenges.

As the USAF continues to develop its cyberforce, the concept of *quality* over *quantity* must be the linchpin of its efforts. At the core of this concept must be a skillset supported by an educational baseline. Corporately, STEM disciplines have produced the cyberspace domain and remain essential to operating or managing each of the functional areas. Though the USAF's realization of the value of STEM degrees is a major stepping-stone, it is not enough. The broad-brush categorization that the STEM "bucket" allows is simply not sufficient. For example mechanical engineering (though preferable over a non-science degree) is not as applicable to network operations in comparison to degrees in computer or electrical engineering. STEM degrees are not equally applicable across each of the functional areas. Simply determining career viability from a degree is poor management of human capital. To best prepare each functional area for mission success, higher-fidelity tailored management is necessary.⁵⁹

⁵⁶ E.g. Human intervention directly affects action(s)

⁵⁷ E.g. Human intervention indirectly affects action(s)

⁵⁸ Dr. Kamal Jabbour, Education of Cyber Officers, 2

⁵⁹ [Recommendation R16](#): Manage the education of accessions by functional area with course (or at least concentration) specificity.

UNCLASSIFIED
Cyberspace Human Capital

Acknowledging the baseline in the fundamentals of cyberspace operations, the USAF currently mandates that 70% of the officers accessed into the 17D career field have an accredited STEM degree relating to Network Operations or Cyber Warfare Operations. The degree must be in the following disciplines: Computer Science, Computer/Electrical Engineering, Applied Physics, Industrial/Electromechanical Engineering, Computer Technology, Cyber Warfare, Mathematics, or Management Information Systems. While this is a step in the right direction, national trends in the number of Americans graduating with STEM degrees make the mandatory target difficult to obtain. To maintain DoD's technological and military superiority, the USAF must reverse this trend by deliberately growing its pool of engineers.⁶⁰ There are a few ways that could significantly increase the human capital inventory:

- 1) The Air Force must take a holistic view when it comes to education and STEM requirements. The vast majority of individuals that enter the USAF do so with the intention to become a pilot. This is perfectly understandable; after all, the genesis mission of the USAF is “To fly, fight and win.” As a prerequisite to undergraduate pilot training (UPT), the USAF should require 70% of applicants to have a STEM degrees.⁶¹ This idea is echoed by Jabbour who states, the prerequisite “provide a first-order effect of an increase in the number of officer candidates pursuing engineering degrees with the goal of securing pilots, increasing the consequently the number of nonrated officers with

⁶⁰ Dr. Kamal Jabbour, “CyberVision and Cyber Force Development,” *Strategic Studies Quarterly*, Spring 2010, 70.

⁶¹ [Recommendation R17](#): Assess the holistic AF requirement for STEM degrees to positively affect 17D throughput.

UNCLASSIFIED
Cyberspace Human Capital

[STEM] degrees.”⁶² Those UPT candidates that medically disqualify or fail to successfully complete UPT are now potential accessions for the cyberspace workforce. Additionally, as pilots achieve senior rank, the USAF will have “more technical leadership educated to deal with the uncertain challenges of the technological age.”⁶³

- 2) Formally institute the direct accession to Air Force Information and Technology Master’s program for the cyberspace officer career field. This designates specific quotas for ROTC and USAF Academy graduates to pursue immediately after commissioning. The quota would ensure degrees align with the appropriate functional areas, and following completion of the Master’s program, individuals will be placed in targeted positions. Additionally, completing a graduate-level degree early in one’s career optimizes the amount of time available for force development.⁶⁴

In instances where trends do not allow the mandatory target accession rate, the 17D career field does allow 30% of its accessions to have non-STEM related degrees or non-cyberspace related STEM degrees (e.g. environmental chemistry). On the surface, this is not concerning, because as noted in the 2013 DoD Cyberspace Workforce Strategy, “not all successful cyberspace personnel will have a [STEM] background.”⁶⁵ However, for others without STEM degrees, it can be quite difficult to complete required training. To ensure this workforce has the knowledge in Network, Information or Electromagnetic Operations prior to

⁶² Jabbour, Kamal, “Cyber Vision and Cyber Force Development,” Strategic Studies Quarterly, 71.

⁶³ Ibid.

⁶⁴ Recommendation R18: Formalize the direct accession to AFIT program for cyberforce officers.

⁶⁵ Department of Defense. *DoD Cyberspace Workforce Strategy*, 2013, 9.

UNCLASSIFIED
Cyberspace Human Capital

initial skills training (IST), it is recommended that the USAF utilize aptitude/affinity testing (mentioned in the Force Management section). Furthermore, aptitude/affinity testing could reduce the “wash-out” rate at IST amongst those without non-cyberspace related STEM degrees.

As the cyberspace workforce moves toward improving baseline skillsets, a solid foundation in cybersecurity is imperative. The Cybersecurity Workforce Improvement Program establishes that graduates of Undergraduate Cyber Training (UCT) will continue to attain Information Assurance Management (IAM) Level I certification (e.g. Security+) as a precondition for matriculation into the career field. In order to demonstrate increased foundational knowledge and continued professional progression, cyberspace Field Grade Officers (FGOs) (O-4 to O-5 ranks) will attain and maintain, at a minimum, an IAM Level II certification (e.g., Certified Information Systems Security Professional (CISSP), or equivalent) regardless of technical or leadership track. Though certifications serve a purpose, they should not be confused with Bachelor and Master level STEM degrees. Certifications are not all created equal. Lower level certifications such as Security+ and A+ are easily achieved through training. To achieve more advanced certifications such as Certified Ethical Hacker, CISSP and Global Security Essentials Certification, an element of education is required. For cyberspace officers to be successful, education must serve as the bedrock to follow-on functional training.

TRAINING

The 17D career field should focus the majority of its weight on training only after providing education in key niche areas. While education underpins the unknown environment

UNCLASSIFIED
Cyberspace Human Capital

that cyberspace professionals will face in the future, training provides the foundation for the issues currently confronting the USAF and the cyberspace domain. “Thinkers” are needed to navigate today’s operational environment and tomorrow’s challenges. The USAF must take educated thinkers and “weaponize” them via an operational training pipeline.

The current cyberspace officer pipeline, undergraduate cyberspace training (UCT), “baselines” accessions through a combination of training and education. A large portion of the six-month course trains students on tactical communications, network fundamentals, ethics and traditional communication systems. The remaining portion of UCT provides students with a broad educational overview on cyberspace operations and the different underlying skillsets. Upon completion of UCT, graduates are expected to become cyberspace operators. However, because the training attempts to bring all students with varying educational starting points up to the same level of knowledge, it falls short in providing in-depth technical knowledge and skill sets. Furthermore, the current construct does not allow students to test out of blocks based on experience or knowledge, which could reduce the amount of time a student spends in IST. To better frame the asymmetric cyberspace environment, UCT training tasks and objectives should be functionally aligned under NetOps, EMO, IO and Cyberspace Maintenance.

The overall intent of IST is to develop skill sets. UCT in its current “baseline” variation fails to achieve this objective. There are a few ideas that could help UCT better meet its objectives and increase the probability of a cyberspace squadron commander receiving a UCT graduate that is nearly mission-qualified:

UNCLASSIFIED
Cyberspace Human Capital

- 1) The initial 6-month baselining process becomes more efficient if the majority of accessions have a STEM background and have passed an aptitude/affinity test.
- 2) Require all UCT students to take an initial assessment to determine if the student can accelerate through training. The assessment can provide “on-ramps” to shorten the training pipeline for those individuals who can demonstrate mastery on tasks and objectives prior to receiving instruction.⁶⁶
- 3) Change the UCT construct to allow the first four months (Phase I and II) to “baseline” students and the last two months to build and focus on job-specific tasks, allowing quicker Mission Qualification Training (MQT) after PCS. These two months become Initial Qualification Training (IQT). To facilitate this change requires the UCT schoolhouse to work with AFPC to release assignments and host “drop night” two and half months earlier. This also helps centralize and standardize IQT.⁶⁷

The USAF must continue to provide the means to practice hard-won technical skills that perish over-time. SAF/CIO’s Information Dominance Flight Plan states that, “The Air Force will deliberately cultivate Cyber[space]-Airmen able to dynamically design, build, engineer and configure within the information environment, defend friendly capabilities and resources from attack through cyberspace, and plan and execute cyberspace operations integrating air-minded expertise to achieve joint/combined forces commander objectives.” SAF/CIO’s vision is on the

⁶⁶ [Recommendation R19](#): Require an initial assessment test on Day 1 of UCT and allow students to “test out” of blocks to shorten training pipeline.

⁶⁷ [Recommendation R20](#): Adjust UCT Phase I to four months and Phase II to two months.

UNCLASSIFIED
Cyberspace Human Capital

mark, but in order to complete this broad range of missions, the Air Force must embrace tools and programs to promote routine exercise of those skills. One example is the implementation of a “Cyberspace-PT” program. Without question, the USAF realizes that continued exercise is crucial to maintaining fit-to-fight Airmen. Similar to the advantages to continued physical training, it is imperative that cyberspace officers maintain currency through exercise of their cyberspace skillset. Cyberspace-PT is comparable to the need for pilots to maintain proficiency through routine. One possible implementation is the use of a points based program (similar to that of the acquisitions career field’s continuous learning points or flight gates) where cyberspace officers are granted the opportunity, and required to maintain, their skill set.

The continuum of learning is an ongoing process that does not end after IST. The process starts at a cyberspace officer’s accession source and continues throughout one’s career. It is important that senior cyberspace leaders persistently emphasize the importance of continued training and certification to maintain cyberspace skill sets and to carry forward into the joint environment. The cyberspace career field does provide a rather robust Professional Continuing Education program designed for officers with core 17D AFSC but open to other cyberspace professionals such as 13S, 14N, 62E, 63A and sister service members. Together Cyber 200, Cyber 300 and Cyber 400 leverage experience and training at the tactical, operational and strategic level to enhance knowledge of cyberspace systems and develop focus to better integrate cyberspace capabilities into the appropriate level of military operations. However, the cyberspace career field needs to allocate resources to stimulating thoughts and ideas on dealing

UNCLASSIFIED
Cyberspace Human Capital

with future and current threats and maintaining perishable skill sets. There are many available avenues to provide this competence:

- 1) Encourage cyberspace officers to participate in cyberspace competitions to add depth to skillsets. Cyberspace competitions provide a venue and an opportunity for cyberspace officers to utilize and improve their skill sets in a closed but dynamic environment. These competitions help to hone their expertise and bolster their affinity for cyberspace.
- 2) Encourage cyberspace officers to participate in wargaming and exercises. Exercises such as Cyber Flag and Cyber Storm serve to validate education and training and to prepare officers against a realistic enemy by fusing attack and defense across the full spectrum of operations. In the dynamic cyberspace environment, wargaming and exercises help to identify individual and organizational training deficiencies. By identifying these shortfalls early and quickly, training can be modified to address the issues.⁶⁸
- 3) Encourage cyberspace officers to compete for premier programs like WIC (Weapons Instructor Course), EWI (Education with Industry), AFIT (Air Force Institute of Technology) and CNODP (Computer Network Operations Development Program), which offer unparalleled paths to excellence. Training and education programs such as these must continue to increase throughput, while not lowering requirements and standards. More often than not, the pool of qualified applicants far surpasses the pipeline

⁶⁸ [Recommendation R21](#): Encourage cyberforce officers to participate in cyberspace symposiums, cyberspace competitions and wargaming/exercises to preserve skill sets and operationalize training.

UNCLASSIFIED
Cyberspace Human Capital

throughput, resulting in missed opportunity. The breadth of experience that graduates of these programs bring to a burgeoning operational area is enormous.⁶⁹

This last recommendation highlights the importance of flexibility within cyberspace. As stated in the Air Force Information Dominance Flight Plan, “CKT changes with the mission and adversary and may exist in many forms (to include links, RF communications, and spectrum) thus requiring a keen awareness and understanding how an adversary operates and how to anticipate their next move.”⁷⁰ This requires cyberspace officers to have a solid educational foundation best provided via a STEM degree as well as training that is continuously examined for new needs and modifications.

FLEXIBILITY

USAF doctrine often reflects the best means to obtain warfighting effects is based on the US' most recent war experience. This experience and wisdom is utilized to develop the training standards and curriculum taught at IST. In the case of cyberspace, the effects must be based in real-time to maintain the US' warfighting edge over its adversaries. In order to build systems that are resilient when attacked, conduct offensive attacks when required, and maintain and protect critical networks, the UCT curriculum needs to be adaptive to meet and respond to current demands in cyberspace. The cyberspace career field does a good job ensuring that the

⁶⁹ [Recommendation R22](#): Revisit throughput levels on specialized programs (e.g. WIC, AFIT, EWI, CNODP etc) in order to determine ways to increase and incentive special skills.

⁷⁰ Air Force Information Dominance Flight Plan, The Way Forward for Cyberspace, May 2015, 13.

UNCLASSIFIED
Cyberspace Human Capital

Professional Continuing Education (PCE) courses and curriculum remains relevant and current in times of rapid change; the same rigor should be applied to UCT.

The Utilization & Training Workshop (U&TW)/Specialty Training Requirements Team Process is the forum that the USAF utilizes to create or to revise training standards and to ensure the validity and viability of career field training. According to AFI 36-2201, *Air Force Training*, the career field manager (CFM) in partnership with the Air Education and Training Command (AETC) Training Pipeline Manager (TPM) and MAJCOM Functional Managers (FM) drive this process. Currently, the 17D CFM under the authority of the Chief, Information Dominance and Chief, Information Officer (also known as the Functional Authority for Cyberspace Operations), holds an annual U&TW to evaluate current training standards and discuss any necessary changes. While it is commendable to host a meeting and make decisions, the intent is lost if the implementation of those decisions takes too long. During the U&TW held in April 2013, several decisions were made which included curriculum modifications to UCT. It took over a year for the results to come to fruition. Together the AETC TPM and the 17D CFM must do a better job of quickly implementing changes to UCT so that students are receiving relevant training.

The following ideas could aid the process:

- 1) Require UCT to conduct an internal, mini U&TW on a biannual basis to identify any necessary changes required to the curriculum based on changes in adversary tactics.

UNCLASSIFIED
Cyberspace Human Capital

Document and send any needed modifications to the CFM for review and consideration.⁷¹

- 2) Employ the USAF Occupational Measurement Squadron to conduct analysis or study to validate that the training standards and material currently taught at UCT is useful.

In other words, are squadron commanders happy with the level of knowledge and skills sets UCT graduates have when they arrive at their units? Is there a skill set that units are having to train to that should be taught at UCT?⁷²

- 3) Similar to the CDC development schedule, the 17D CFM should establish overarching curriculum timetables for planning purposes. For example, minor curriculum revision is 30 days; simple revision is 45 days; major revision (typical) is 60 days; and complicated revision is 75 days. This ensures timely implementation of decisions made at the U&TW to modify course material.⁷³

In addition to ensuring relevant course material, the 17D career field must remain open to changing institutional structures that restrict the ability to grow and develop cyberspace leaders. This includes enforcing back-to-back operational tours for new accessions to ensure return on investment on training especially for NetOps as well as loosening the 4-5 year time on station restriction in locations and units that can provide natural career progression. It is the cyberspace

⁷¹ [Recommendation R23](#): Biannually require UCT to conduct an internal U&TW to identify out-dated course material

⁷² [Recommendation R24](#): Require MAJCOM to solicit feedback from units to validate training standards.

⁷³ [Recommendation R25](#): 17D CFM establish development timetables for curriculum revisions to ensure timely implementation.

UNCLASSIFIED
Cyberspace Human Capital

career field's job to prepare its officers for leadership by optimizing experiences and skills and by developing capabilities to meet today's and tomorrow's challenges.

CONCLUSION

Secretary of Defense Ashton Carter recently characterized the challenges of the changing national security landscape: "Today's security environment is dramatically different than the one we've been engaged in for the last 25 years and it requires new ways of thinking and new ways of acting."⁷⁴ More than ever before, assuring mission success in contemporary operations will inevitably integrate elements of cyberspace. Cyberspace operations, unilaterally or in support of air, sea, land, human and space missions, serve as the protagonist to 21st century national security. Game-changing technological advancements and innovative low-cost adaptive solutions continue to change the landscape of the cyberspace key terrain. Furthermore, defending cyberspace is not a solitary effort that can be tasked to single entity; unitary efforts that bring service components, government institutions and partner nations together are the mainstay of efforts for the foreseeable future. It is clear that the United States is entering a new strategic era that stems from changing social, political and economic trends. In order to ensure that the United States maintains decision dominance and battlespace superiority, efforts must keep up with, and run parallel to, the changes ahead.

In order to sustain the United States' edge in future conflicts, USAF leadership must develop a sustainable and flexible framework that manages and develops cyberspace cadre,

⁷⁴ Secretary of Defense Ash Carter, [comments with respect to the recent release of the President's FY 17 Defense Budget](#)

UNCLASSIFIED
Cyberspace Human Capital

today and into the future. It must consider the force of the future holistically, using a cradle-to-grave approach to secure the talent necessary to assure mission success in cyberspace; accessions and retention are equal-weight tasks in ensuring an effective human capital plan for decades to come. The USAF must also revisit how it manages and develops cyberspace operators by adapting a functional specific model that mirrors the characteristics of the cyberspace domain (i.e., electromagnetic, information, network and maintenance aspects) over legacy institutional structure. In order to build information age cyberspace human capital, effective force management principles must determine how and where knowledge, skills, and experience are distributed across the force of the future. Additionally, creating a cyberspace cadre that is constantly relevant to information age operations requires agile force development processes that inculcate bottom-up changes that match specific skills, specialties and classification structures with Air Force missions. The challenges are colossal, but as Napoleon once said, “victory belongs to the most persevering.” Given that USAF Airmen are the most innovative and forward-thinking warriors of today’s age, victory will soon belong to us.

UNCLASSIFIED
Cyberspace Human Capital

APPENDIX 1: RECOMMENDATIONS SUMMARIZED

R1: Manage the cyberspace career field through functional subareas

PRO: Functional sub-areas address the four primary operational areas of cyberspace operations vs. groupings based on technology (which changes) or organizational structures (e.g. personnel systems which are inflexible).

CON: Definition of operations runs perpendicular to joint doctrine (e.g. traditionally defined as OCO, DCO, NetOps) and is counter-culture.

R2: Revisit entry requirements by assessing aptitude and affinity as equal indicators of career success.

PRO: Accessions and crossflows are gained based on the merits of BOTH aptitude and affinity, vs.

using STEM + professional certification as the only indicator of success.

CON: Creates a rigor in developing an assessment process that tests and measures aptitude and affinity.

R3: USAF pursue educator investment strategies that amplify recruitment capabilities.

PRO: Tapping into educators will amplify recruitment strategies; educators are involved in “job placement” strategies.

CON: Requires additional recruitment effort that parallels normal ROTC/OTS efforts.

R4: Target NSA academic excellence institutions for accessions

PRO: By targeting those institutions with renowned success in developing cyberspace professionals the

USAF can ensure that the right accessions (with aptitude and affinity) enter service. Targeting efforts would include marketing strategies directed at those institutions with scholarship opportunities outside of normal channels.

CON: Requires a new program that deliberately targets certain individuals with specific potentials and the allocation of resources (scholarships and mentoring/advising) to those individuals.

R5: Cyberspace alumni profiles in college publications.

PRO: Enhances recruitment message by establishing a mode for potential candidates to engage with current cyberspace officers; stories inspire potential candidates.

UNCLASSIFIED
Cyberspace Human Capital

CON: Requires time/investment to craft a public relations targeted message.

R6: USAF develop specific accession strategies necessary to target and recruit talent.

PRO: Deliberately targets specific educational, aptitude and affinity necessary to fill functional areas (EW, NetOps, IO) through accession strategies; opens the talent pipeline for the cyberspace force of the future.

CON: ROI may not be realized until periods following initial 10 years commitment: Financial & time investment is required and will only pay dividends if commitment to new accession strategy is persistent; it must become an institutional norm.

R7: Retain cyberspace operations officers by supporting technology passions

PRO: Retain the cyberspace operations officer through supporting technology proficiency.

CON: Costs of TDY/time away from core mission.

R8: Retain cyberspace operations officers by facilitating exposure opportunities

PRO: Retain the cyberspace operations officer through networking and developing partnerships.

CON: Costs of TDY/time away from core mission.

R9: Develop a selective USAF cyber-conference

PRO: Retain the cyberspace operations officer through supporting technology proficiency.

CON: Costs of TDY/time away from core mission.

R10: Revisit/revise career path (pyramid) for cyberspace officers

PRO: Provides career agility by ensuring that cyberspace officers have either a technical or a management track with merit-based promotion opportunity.

CON: Revise current career path (pyramids) which is counter-cultural to USAF processes and may impact promotion boards across the USAF.

R11: Develop a tiered “in-rank” bonus system to encourage continuation of service along technical tracks.

PRO: Fosters a means to enable those with aptitude/affinity for the technical side of cyberspace operations to continue service (prevents “up or out” promotions). Serves the needs of the USAF by ensuring knowledge, skills and ability are retained in service.

CON: Necessary monetary incentives that drive another bill for a fiscally constrained USAF.

UNCLASSIFIED
Cyberspace Human Capital

R12: Conduct exit interviews to discern why cyberspace operations officers separate from service.

PRO: Exposing and collecting data on why cyberspace operations officers leave active service can help address the right problem with the right solution. The “easy” assumption to make is that officers separate due to financial reasons; however, this may not always be the case.

CON: Resources (time) will have to be spent to form an exit interview that asks the right questions.

R13: Expose cyberspace officers to joint environments early in their careers.

PRO: Exposing USAF cyberspace officers to joint operations early on enables flexibility in operations and leverages knowledge, skills and experience across the entire force.

CON: Revising career and development milestones is challenging to formalize for a 2,500+ career field.

R14: Lower barriers for crossflow into cyberspace operations for those with the requisite knowledge, skills and experience.

PRO: Maximizes knowledge, skills and experience from talent across the Air Force

CON: Will run counter to personnel systems which often seek to “protect” manning slots instead of seeking best needs of the Air Force.

R15: Leverage human capital across the ANG/AF Reserves to maximize force capabilities

PRO: Taps potential human capital in the ANG/AF that is not inherent to the AD force. ANG/AF often bring niche skills and experience (from civilian life) that would promote cyberspace mission assurance.

CON: Will run counter to ANG/AF Reserve manpower requirements, which might resist the transfer of their talent to the AD force. Additionally, ANG/AF Reserve personnel may not volunteer to assume AD duties because of the benefits of working on the ANG/AF Reserve force (stability, lower ops-tempo etc).

R16: Manage the education of accessions by functional area with course (or at least concentration) specificity.

PRO: Increases eligible cyberspace officer pool, and, potentially, technically competent senior leaders.

CON: Requires additional management oversight.

UNCLASSIFIED
Cyberspace Human Capital

R17: Assess the holistic AF requirement for STEM degrees to positively affect 17D throughput.

PRO: Increases eligible cyberspace officer pool and increase the number of technically competent senior leaders.

CON: Tougher prerequisites for UPT applicants.

R18: Formalize the direct accession to AFIT program for cyberspace officers.

PRO: Increases the number of cyberspace officers with a solid educational foundation in engineering and shortens pipeline training.

CON: Delays entrance into tactical level unit by two years and current PME policy does not allow AFIT degrees obtained outside of the eligible IDE window to receive equivalency credit.

R19: Require an initial assessment test on Day 1 of UCT and allow students to “test out” of blocks to shorten training pipeline.

PROS: Potentially shortens the amount of time student spends in training and identifies officers that have skill sets that usually take longer to train. These students are ideal for NetOps jobs that have long MQTs because they can exit the pipeline sooner and enter a unit and begin MQT process.

CONS: Students do not benefit from the experience and expertise of other students.

R20: Adjust UCT Phase I to four months and Phase II to two months.

PROS: Uses STEM foundation to speed along baseline training, allows career field to develop skill sets because Phase II will function as IQT/MQT and sends graduates to units that are almost MQT.

CONS: CFM will have to spend resources to modify training program.

R21: Encourage cyberspace officers to participate in cyberspace symposiums, cyberspace competitions and wargaming/exercises to preserve skill sets and operationalize training.

PROS: Validates education and training, serves to incentivize cyberspace operators to hone skill sets and potentially helps in the recruitment of future cyberspace officers.

UNCLASSIFIED
Cyberspace Human Capital

CONS: Resource allocation and time spent outside the unit.

R22: Revisit throughput levels on specialized programs (e.g. WIC, AFIT, EWI, CNODP etc.) in order to determine ways to increase and incentive special skills.

PROS: Premier programs (e.g. WIC, AFIT, EWI, CNODP, etc.) turn applicants away based on quota and not qualifications. By opening the aperture (and NOT lowering requirements) more cyberspace officers could be developed with critical skills.

CONS: Perception of doing injury to these programs by accepting more applicants.

R23: Biannually require UCT to conduct an internal U&TW to identify out-dated course material.

PROS: Forces UCT schoolhouse to assess the relevancy of course material on a more regular basis.

CONS: Potentially resource heavy.

R24: Require MAJCOM to solicit feedback from units to validate training standards.

PROS: Allows squadron-level participation in determining training standards

CONS: Allows squadron-level participation in determining training standards

R25: 17D CFM establish development timetables for curriculum revisions to ensure timely implementation.

PROS: Quicker implementation of curriculum and training standard revisions.

CONS: Manpower and resource allocation to maintain long-term commitment.